REMARKS

The Examiner has rejected Claim 14 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner has stated that "Claim 14 recites the limitation 'third file format' and 'fourth file format' in the first and second element have not been defined."

Applicant respectfully disagrees and emphasizes that Claim 14 is dependent upon Claim 1, which describes an "electronic file having a first file format," and "converting the certain electronic file to a second file format" (emphasis added), as claimed. Thus, applicant's claimed "second electronic file having a third file format," and "converting the second electronic file to a fourth file format" (emphasis added), as claimed in Claim 14, is definite.

The Examiner has rejected Claims 1-10, 12-16, 18-21, 24-30, 32-34 and 35-39 under 35 U.S.C. 102(e) as being anticipated by Stewart et al. (U.S. Patent No. 6,901,519). In addition, the Examiner has rejected Claims 17, 22, 23 and 40 under 35 U.S.C. 103(a) as being unpatentable over Stewart, in view of Nachenberg et al. (U.S. Publication No. 2003/0088680). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claim 22.

With respect to the independent Claims 1, 28, and 36, the Examiner has relied upon Col. 3, lines 56-64 from the Stewart reference to make a prior art showing of applicant's claimed "converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format" (see this or similar, but not necessarily identical language in the aforementioned independent claims).

> "If the e-mail contains an attachment with an extension that is not in either the 'disapproved' or 'approved' lists, the entire attachment is passed through a conversion process (205) that eliminates all executable code leaving only alphanumeric message text. This process will generally create a readable copy of the attachment, but will not allow the attachment to open any processes or applications, including executable virus code." (Col. 3, lines 56-64 - emphasis added).

Applicant respectfully asserts that the excerpt from Stewart relied upon by the Examiner merely discloses that "[i]f the e-mail contains an attachment with an extension that is not in either the 'disapproved' or 'approved' lists, the entire attachment is passed through a conversion process (205) that eliminates all executable code leaving only alphanumeric message text" (emphasis added). However, merely eliminating all executable code leaving only alphanumeric message text for an attachment with an extension not in the disapproved or approved lists, as in Stewart, fails to suggest "converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format" (emphasis added), as claimed by applicant. Clearly, removing executable code leaving only alphanumeric message text, as in Stewart, simply fails to even suggest "converting...to a second file format having a second file extension that is different from the first file extension" (emphasis added), as claimed by applicant.

With respect to the subject matter of former Claim 22 (now at least substantially incorporated into each of the independent claims), the Examiner has relied on Paragraphs [0003] and [0051] from the Nachenberg reference to make a prior art showing of applicant's claimed technique "wherein it is determined if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the first file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG

file format if it is determined that the first file format is the graphics file format type" (see this or similar, but not necessarily identical language in the independent claims).

> "A computer virus, in the broad sense that the term is used in the present specification and claims, is any malicious computer program or code that has the potential to infect normal computer files or damage computer systems in any way. Computer viruses typically reside in executable computer code and are activated when the computer code is executed. For example, a computer virus may be buried in an .EXE or .COM file, a Java script file embedded in an email in HTML format, or a WORD macro template, etc. Some computer viruses replicate themselves to use up computer resources in computer hard drives or memories and thus cause the computer system to collapse. Some computer viruses reformat computer hard drives to destroy computer files. Some computer viruses do not copy themselves to other computer code, e.g., Trojan horse type viruses, but they allow a hacker in a remote computer to take control of an infected computer." (Nachenberg, Paragraph [0003] – emphasis added)

> "In alternative embodiments, besides performing access control functions as commanded by access control message 202, access control module 203 may also perform other functions to protect computer network 1. For example, if access control module 203 is installed on an E-mail gateway server 3 of computer network 1, it performs E-mail filtering functions for computer network 1. When access control system 200 enters into an alert mode warning of an imminent virus attack, access control module 203 automatically filters all incoming E-mails for executable file attachments, such as .EXE, .VBS, .JS files. The result of the filtering is to allow the E-mail bodies to be forwarded to recipients 2, 3 but to strip all executable attachments from the E-mails. For example, all the embedded Java script or VBS script code encoded in HTML mail bodies are automatically removed; and all the macros from incoming documents, spreadsheets, and PowerPoint presentation files are also removed." (Nachenberg, Paragraph [0051] – emphasis added)

Applicant respectfully points out that the Nachenberg excerpts relied upon by the Examiner merely teach that "a computer virus may be buried in an .EXE or .COM file, a Java script file embedded in an email in HTML format, or a WORD macro template" and that the access control module "filters all incoming E-mails for executable file attachments" and "strip[s] all executable attachments from the E-mails," so that potential viruses are "automatically removed" (Nachenberg, Paragraphs [0003] and [0051]).

However, applicant respectfully asserts that generally disclosing that "a computer virus may be buried in an .EXE or .COM file, a Java script file embedded in an email in HTML format, or a WORD macro template," in addition to using an access control module that "filters all incoming E-mails for executable attachments," and then "strip[s] all executable attachments," as in Nachenberg, in no way teaches or suggests applicant's claimed technique "wherein it is determined if the first file format is one of a word processing file format type and a graphics file format type, the **second file format** being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts **if it is determined that the first file format is the word processing file format type**, the **second file format** being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format **if it is determined that the first file format is the graphics file format type**" (emphasis added), as claimed by applicant. Clearly, stripping an executable attachment from an E-mail to eliminate a virus, as in Nachenberg, fails to teach "the second file format... if it is determined that the first file format is the word processing file format type" or "the second file format...if it is determined that the first file format is the graphics file format type," in the manner as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Therefore,

a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 7, as rejected under 35 U.S.C. 102(e), the Examiner has relied on Col. 4, lines 18-20 from the Stewart reference to make a prior art showing of applicant's claimed "converting occurring at a desktop computer of the intended recipient."

> "If the attachments contain unapproved macros, the attachment is forwarded to an available sacrificial PC processor (103) via data link (108) for conversion to a non-executable format and further detailed virus testing." (Stewart, Col. 4, lines 17-21 - emphasis added)

Applicant respectfully points out that the Stewart excerpt relied upon by the Examiner teaches the use of "a sacrificial PC processor" for "conversion to a non-executable format and further detailed virus testing" following the conversion of the attachment (Stewart, Col. 4, line 19 – emphasis added). Furthermore, Stewart discloses that "[s]acrificial PC processing begins with the original e-mail attachment being passed to an available sacrificial PC (105) via a data link (108) connecting the Gatekeeper server (102) with the sacrificial PC" (Col. 4, lines 29-32 – emphasis added).

However, applicant respectfully asserts that the use of a "sacrificial PC processor" for "conversion and further detailed virus testing," where the original email attachment is passed to the sacrificial PC via a data link connecting the Gatekeeper server with the sacrificial PC, as in Stewart, in no way teaches that the "converting occur[s] at a desktop computer of the intended recipient" (emphasis added), as claimed by applicant. Clearly, passing the email attachment to the sacrificial PC via a data link, as in Stewart, simply fails to suggest that "converting occur[s] at a desktop computer of the intended recipient" (emphasis added), as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 41-44 below, which are added for full consideration:

> "wherein said converting replaces formatting of the certain electronic file with new formatting to retain an original appearance of the certain electronic file" (see Claim 41);
>
> "wherein a notification indicating the certain electronic file represents a potential security risk is sent to the intended recipient in response to the determination that the certain electronic file represents at least the potential risk to the security of the computer system" (see Claim 42);
>
> "wherein a server computer forwards the converted electronic file to the intended recipient in response to a request to view the certain electronic file from the intended recipient" (see Claim 43); and
>
> "wherein a desktop computer of the intended recipient performs said converting of the infected electronic file to the second file format prior to the user opening the certain electronic file" (see Claim 44).

Again, a notice of allowance or a proper prior art showing of <u>all</u> of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P092).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100